REVISED SECURITY PROCEDURES ESTABLISHED PURSUANT TO PUB. L. 96–456, 94 STAT. 2025, BY THE CHIEF JUSTICE OF THE UNITED STATES FOR THE PROTECTION OF CLASSIFIED INFORMATION

1. **Purpose.** The purpose of these procedures, as revised, is to meet the requirements of Section 9(a) of the Classified Information Procedures Act of 1980, Pub. L. 96–456, 94 Stat. 2025, as amended ("the Act"), which in pertinent part provides that:

> ". . . [T]he Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. . . ."

These revised procedures apply in all criminal proceedings involving classified information, and appeals therefrom, before the United States district courts, the courts of appeal and the Supreme Court, and supersede the Security Procedures issued on February 12, 1981.

2. **Classified Information Security Officer.** In any proceeding in a criminal case or appeal therefrom in which classified information is within, or is reasonably expected to be within, the custody of the court, the court will designate a "classified information security officer." The Attorney General or the Department of Justice Security Officer will recommend to the court a person qualified to serve as a classified information security officer. This individual will be selected from the Litigation Security Group, Security and Emergency Planning Staff, Department of Justice, to be detailed to the court to serve in a neutral capacity. The court may designate, as required, one or more alternate classified information security officers who have been recommended in the manner specified above.

The classified information security officer must be an individual with demonstrated competence in security matters. Prior to designation, the Department of Justice Security Officer must certify in writing that the classified information security officer is properly cleared, i.e., possesses the necessary clearance for the level and category of classified information involved.

The classified information security officer will be responsible to the court for the security of all classified information in the court's custody, including, but not limited to, any pleadings or other filings created in connection with the proceedings, and any form of information contained in any format, including testimony, notes, photographs, transcripts, documents, digital files, audio files or video files, stored on any type of equipment (e.g., computers, electronic storage devices, etc.). In addition, any matters relating to personnel, information, or communications security will be the responsibility of the classified information security officer who will take measures reasonably necessary to fulfill these responsibilities. The classified information security officer must notify the court and the Department of Justice Security Officer of any actual, attempted, or potential violation of security procedures.

3. **Secure Location.** Any *in camera* proceeding—including, but not limited to, a pretrial conference, motion hearing, status hearing, suppression hearing, substitution hearing, or appellate proceeding—concerning the use, relevance, or admissibility of classified information must be held in a secure location recommended by the classified information security officer and approved by the court.

The secure location must be within the federal courthouse, unless it is determined that no available location in the courthouse meets, or can reasonably be adapted to meet, the security requirements of the Executive Branch applicable to the level and category of classified information involved. In the event that no suitable location exists within the courthouse, upon recommendation by the classified information security officer, the court will designate another United States Government facility located within the vicinity of the courthouse, as the secure location.

The classified information security officer must make necessary arrangements to ensure that the security requirements of the Executive Branch applicable to the level and category of classified information involved are met and must conduct or arrange for such inspection of the secure location as may be necessary. The classified information security officer must, in consultation with the United States Marshal, arrange for the installation of security devices and take such other measures as may be necessary to protect against any unauthorized access to or disclosure of classified information. All of the aforementioned activities must be conducted in a manner that does not interfere with the orderly proceedings of the court. Prior to any hearing or other proceeding, the classified information security officer must certify to the court that the location to be used is secure.

4. **Personnel Security—Court Personnel.** No person appointed by the court or designated for service therein will be given access to any classified information in the custody of the court, unless such person has received the appropriate security clearance and unless access to such information is necessary for the performance of an official function. A security clearance for justices and other Article III judges is not required.

The court shall timely notify the classified information security officer of the names of court personnel who may require access to classified information. The classified information security officer will then notify the Department of Justice Security Officer, who will promptly make arrangements to obtain any necessary security clearances. All security clearance requests will be reviewed and determinations will be made in accordance with the adjudication standards of the Executive Branch applicable to the level and category of classified information involved. The classified information security officer, on behalf of the Department of Justice Security Officer, will advise the court when the necessary security clearances have been obtained. When necessary, the court may request that security clearances for certain court personnel be expedited.

If security clearances cannot be obtained promptly, United States Government personnel possessing the appropriate security clearances may be temporarily assigned to assist the court. If a proceeding is required to be recorded and an official court reporter having the necessary security clearance is unavailable, the court may request the classified information security officer or the attorney for the government to have a cleared reporter designated to act as a reporter in the proceedings. The reporter so designated must take the oath of office as prescribed by 28 U.S.C. § 753(a).

Justices, judges and cleared court personnel may disclose classified information only to persons who possess both the appropriate security clearance and the requisite need to know the information in the performance of an official function. However, nothing contained in these procedures precludes a judge from performing his or her official duties, including giving appropriate instructions to a jury.

Any security concern regarding classified information and involving court personnel or persons acting for the court must be referred to the court and the Department of Justice Security Officer for appropriate action.

5. **Persons Acting for the Defense.** The government may obtain information by any lawful means concerning the trustworthiness of persons associated with the defense and may bring such information to the attention of the court for the court's consideration in framing an appropriate protective order pursuant to Section 3 of the Act.

6. **Jury.** Nothing contained in these procedures will be construed to require an investigation or security clearance of the members of a jury or to interfere with the functions of a jury, including access to classified information introduced as evidence in the trial of a case.

At any time during trial, the trial judge should consider, based on a party request or sua sponte, giving the jury a cautionary instruction regarding the release or disclosure of any classified information provided to the jury.

7. **Custody and Storage of Classified Materials.**

a. Materials Covered. These security procedures apply to any classified information, as the term is defined in Section 1(a) of the Act, that is in the custody of the court. This includes, but is not limited to any pleadings or other filings created in connection with the proceedings, and any form of information contained in any format, such as testimony, notes, photographs, transcripts, documents, digital files, audio files or video files, stored on any type of equipment (*e.g.*, computers, electronic storage devices, etc.).

b. Safekeeping. Classified information submitted to the court must be placed in the custody of the classified information security officer or appropriately cleared court personnel who will then be responsible for its safekeeping. When not in use, all classified materials must be stored in a safe that conforms to the General Services Administration standards for security containers. Classified information will be segregated from other information unrelated to the case at hand by securing it in a separate security container. If the court does not possess a storage container that meets the required standards, the necessary storage container or containers are to be supplied to the court on a temporary basis by the appropriate Executive Branch agency as determined by the Department of Justice Security Officer. Only the classified information security officer, alternate classified information security officer(s), and appropriately cleared court personnel will have access to the combination and the contents of the container.

For other than temporary storage (e.g., a brief court recess), the classified information security officer must ensure that the storage area in which these containers will be located meets Executive Branch standards applicable to the level and category of classified information involved. The secure storage area may be located within either the federal courthouse or the facilities of another United States Government agency.

c. Transmittal of Classified Information. During the pendency of any hearing, trial or appeal, classified materials stored in the facilities of another United States Government agency must be transmitted to and from the court in the manner prescribed by the Executive Branch security regulations applicable to the level and category of classified information involved. A trust receipt must accompany all classified materials transmitted and must be signed by the recipient and returned to the classified information security officer.

8. Operating Routine.

a. Access to Court Records. Court personnel will have access to court records containing classified information only as authorized. Access to classified information by court personnel will be limited to the minimum number of cleared persons necessary for operational purposes. Access includes presence at any proceeding during which classified information may be disclosed. Arrangements for access to classified information in the custody of the court by court personnel and by persons acting for the defense must be approved in advance by the court, which may issue a protective order concerning such access.

b. Access to Other Discoverable Information. Except as otherwise authorized by a protective order, persons acting for the defense will not be given custody of classified information provided by the government. They may, at the discretion of the court, be afforded access to classified information provided by the government in secure locations that have been approved in accordance with § 3 of these procedures, but such classified information must remain in the control of the classified information security officer. The classified information security officer also will control access to classified information in the possession of the defense that is filed with the court or is reasonably expected to come within the custody of the court.

c. Telephone and Computer Security. Classified information must not be discussed, communicated, or processed using any non-secure communication device including standard commercial telephone instruments or office intercommunication systems, cellular devices, computers, and/or other electronic or internet-based communication services. Classified information may only be discussed, communicated and processed on devices cleared for the level of classification of the information to be disclosed or processed as approved by the Classified Information Security Officer.

d. Disposal of Classified Material. The classified information security officer is responsible for the secure disposal of all classified materials in the custody of the court which are not otherwise required to be retained.

9. Records Security.

a. Classification Markings. The classified information security officer, after consultation with the appropriate classification authority, is responsible for marking all court materials containing classified information with the appropriate level of classification, and for indicating thereon any special access controls that also appear on the face of the material from which the classified information was obtained or that are otherwise applicable.

Any and all materials potentially containing classified information filed by the defense must be filed under seal with the classified information security officer. The classified information security officer may permit counsel to file, on the public docket, non-substantive pleadings or documents (*e.g.*, motions for extension of time, scheduling matters, continuances, etc.) that do not contain information that is or may be classified. The classified information security officer must promptly coordinate with the appropriate classification authority to determine whether each filing contains classified information. If it is determined that the filed material does contain classified information, the classified information security officer must ensure that it is marked with the appropriate classification markings. If it is determined that the filed material does not contain classified information, it should be unsealed and placed in the public record. Upon the request of the government, the court may direct that any filed materials containing classified information must thereafter be maintained in accordance with § 7 of these procedures.

b. Accountability System. The classified information security officer is responsible for the establishment and maintenance of a control and accountability system for all classified information received by or transmitted from the court. Upon request, the classified information security officer will provide to the court an inventory of all classified information received by the court.

10. Transmittal of the Record on Appeal. The record on appeal, or any portion thereof, which contains classified information must be transmitted to the court of appeals or to the Supreme Court in the manner specified in § 7(c) of these procedures.

Any court records containing classified information must be maintained, through the pendency of any direct appeal, at a secure location that is reasonably accessible and approved by the classified information security officer, and must be stored in a proper security container.

11. Final Disposition. Within a reasonable time after all proceedings in the case have been concluded, including appeals, the court will release to the classified information security officer all materials containing classified information. The classified information security officer will then transmit them to the Department of Justice Security Officer to be maintained in accordance with approved storage procedures. The materials must be transmitted in the manner specified in § 7(c) of these procedures and must be accompanied by the appropriate accountability records required by § 9(b) of these procedures.

12. Expenses. All expenses of the United States Government that arise in connection with the implementation of these procedures, including any construction or equipment costs, will be borne by the Department of Justice and other appropriate Executive Branch agencies whose classified information is being protected.

13. Interpretation. Any question concerning the interpretation of any security requirement contained in these procedures will be resolved by the court in consultation with the Classified Information Security Officer who will consult with the Department of Justice Security Officer, if necessary.

14. **Term.** These revised procedures remain in effect until modified in writing by The Chief Justice after consultation with the Attorney General of the United States, the Director of National Intelligence, and the Secretary of Defense.

15. **Effective Date.** These revised procedures become effective forty-five days after the date of submission to the appropriate Congressional Committees, as required by the Act.

Effective this 15th day of January, 2011, having taken into account the views of the Attorney General of the United States, the Director of National Intelligence, and the Secretary of Defense, as required by law.

[The revised security procedures set out above were issued Dec. 1, 2010, by John G. Roberts, Jr., Chief Justice of the United States. Prior security procedures were issued Feb. 12, 1981, by Warren E. Burger, Chief Justice of the United States.]

§ 9A. Coordination requirements relating to the prosecution of cases involving classified information

(a) Briefings required.—The Assistant Attorney General for the Criminal Division or the Assistant Attorney General for National Security, as appropriate, and the appropriate United States attorney, or the designees of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified information that originated in the agency of such senior agency official.

(b) Timing of briefings.—Briefings under subsection (a) with respect to a case shall occur—

(1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and

(2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.

(c) Senior agency official defined.—In this section, the term "senior agency official" has the meaning given that term in section 1.1 of Executive Order No. 12958.

(Pub.L. 96–456, § 9A, as added Pub.L. 106–567, Title VI, § 607, Dec. 27, 2000, 114 Stat. 2855; amended Pub.L. 109–177, Title V, § 506(a)(8), Mar. 9, 2006, 120 Stat. 248.)

HISTORICAL AND STATUTORY NOTES

References in Text

Executive Order No. 12958, referred to in subsec. (c), which was set out as a note under 50 U.S.C.A. § 435 (now section 3161), was revoked by Ex. Ord. No. 13526, § 6.2(g), Dec. 29, 2009, 75 F.R. 731.

§ 10. Identification of information related to national defense

In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.

(Pub.L. 96–456, § 10, Oct. 15, 1980, 94 Stat. 2029.)

§ 11. Amendments to Act

Sections 1 through 10 of this Act may be amended as provided in section 2076, Title 28, United States Code.

(Pub.L. 96–456, § 11, Oct. 15, 1980, 94 Stat. 2029.)

HISTORICAL AND STATUTORY NOTES

References in Text

This Act, referred to in catchline, is Pub.L. 96–456, Oct. 15, 1980, 94 Stat. 2025, known as the "Classified Information Procedures Act".

§ 12. Attorney General guidelines

(a) Within one hundred and eighty days of enactment of this Act, the Attorney General shall issue guidelines specifying the factors to be used by the Department of Justice in rendering a decision whether to prosecute a violation of Federal law in which, in the judgment of the Attorney General, there is a possibility that classified information will be revealed. Such guidelines shall be transmitted to the appropriate committees of Congress.

(b) When the Department of Justice decides not to prosecute a violation of Federal law pursuant to subsection (a), an appropriate official of the Department of Justice shall prepare written findings detailing the reasons for the decision not to prosecute. The findings shall include—

(1) the intelligence information which the Department of Justice officials believe might be disclosed,

(2) the purpose for which the information might be disclosed,

(3) the probability that the information would be disclosed, and

(4) the possible consequences such disclosure would have on the national security.

(Pub.L. 96–456, § 12, Oct. 15, 1980, 94 Stat. 2029.)

HISTORICAL AND STATUTORY NOTES

References in Text

The enactment of this Act, referred to in subsec. (a), means Oct. 15, 1980.

§ 13. Reports to Congress

(a) Consistent with applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches, the Attorney General shall report orally or in writing semiannually to the Permanent Select Committee on Intelligence of the United States House of Representatives, the Select Committee on Intelligence of the United States Senate, and the chairmen and ranking minority members of the Committees on the Judiciary of the Senate and House of Representatives on all cases where a decision not to prosecute a violation of Federal law pursuant to section 12(a) has been made.

(b) In the case of the semiannual reports (whether oral or written) required to be submitted under subsection (a) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947.

(c) The Attorney General shall deliver to the appropriate committees of Congress a report concerning the operation and effectiveness of this Act and including suggested amendments to this Act. For the first three years this Act is in effect, there shall be a report each year. After three years, such reports shall be delivered as necessary.